IN THE CLAIMS

1. (Previously Presented) A computer program product for automatically determining if a packet is a new, exploit candidate, the computer program product comprising:

a computer-readable tangible storage device;

first program instructions to determine if the packet is a known exploit;

second program instructions to determine if the packet is addressed to a broadcast IP address of a network;

third program instructions to determine if the packet is network administration traffic;

fourth program instructions, responsive to the packet being a known exploit OR the packet being addressed to a broadcast IP address of a network OR the packet being network administration traffic, to determine that the packet is not a new, exploit candidate; and

fifth program instructions, responsive to the packet not being a known exploit AND the packet not being addressed to a broadcast IP address of a network AND the packet not being network administration traffic AND the packet not being another type of traffic known to be benign, to determine and report that the packet is a new, exploit candidate; and wherein

the first, second, third, fourth and fifth program instructions are stored on the computer-readable tangible storage device.

2. (Previously Presented) The computer program product of claim 1 further comprising:

sixth program instructions to determine if the packet is web crawler traffic; and wherein

the fourth program instructions are responsive to the packet being a known exploit OR the packet being addressed to a broadcast IP address of a network OR the packet being network administration traffic OR the packet being web crawler traffic, to determine that the packet is not a new, exploit candidate; and

the fifth program instructions are responsive to the packet not being a known exploit AND the packet not being addressed to a broadcast IP address of a network AND the packet not being network administration traffic AND the packet not being web crawler traffic, to determine that the packet is a new, exploit candidate; and

the sixth program instructions are stored on the computer-readable tangible storage device.

3. (Previously Presented) The computer program product of claim 1 wherein the first program instructions determine if the packet is a known exploit by searching the packet for a known signature of a known exploit.

4. (Previously Presented) The computer program product of claim 1 wherein the first program instructions determine if the packet is a known exploit by comparing an identity of the packet to one or more identities, sent by an intrusion detection system, of respective packet(s) which the intrusion detection system determined to contain a known exploit.

5. (Previously Presented) The computer program product of claim 1 wherein the packet was received by a honeypot computing device at an unused IP address, and the computer program product is installed and executed at the honeypot computing device.

6. (Previously Presented) The computer program product of claim 1 further comprising:

sixth program instructions, responsive to the fifth program instructions determining that the packet is a new exploit candidate, to determine a signature of the packet, and report the new exploit candidate and the signature to an administrator; and wherein

the sixth program instructions are stored on the computer-readable tangible storage device.

7. (Previously Presented) The computer program product of claim 6 wherein responsive to the fourth program instructions determining that the packet is not a new, exploit candidate, a signature of the packet not being determined.

8. (Previously Presented) The computer program product of claim 1 wherein the second program instructions determine if the packet is addressed to a broadcast IP address of the network by comparing a destination IP address of the packet to a gateway IP address of the network and a netmask of the network which identifies a broadcast IP address of the network.

9. (Currently Amended) A computer program product for automatically determining if a packet is a new, exploit candidate, the computer program product comprising:

a computer-readable tangible storage device;

first program instructions to determine if the packet is a known exploit;

second program instructions to determine if the packet is addressed to a broadcast IP address of a network;

third program instructions to determine if the packet is network administration traffic;

fourth program instructions, responsive to the packet being a known exploit OR the packet being addressed to a broadcast IP address of a network OR the packet being network administration traffic, to determine that the packet is not a new, exploit candidate; and

fifth program instructions, responsive to the packet not being a known exploit AND the packet not being addressed to a broadcast IP address of a network AND the packet not being network administration traffic AND the packet not being another type of traffic known to be benign, to determine and report that the packet is a new, exploit candidate; and wherein

the first, second, third, fourth and fifth program instructions are stored on the computer-readable tangible storage device;

~~The computer program product of claim 1 wherein:~~

the second program instructions also determine if the packet has a protocol listed in a list of protocols previously determined to be harmless network broadcast traffic;

the fourth program instructions are responsive to the packet being a known exploit OR the packet being addressed to a broadcast IP address of a network OR the packet

being network administration traffic OR the packet having a protocol listed in a list of protocols previously determined to be harmless network broadcast traffic, to determine that the packet is not a new, exploit candidate; and

the fifth program instructions are responsive to the packet not being a known exploit AND the packet not being addressed to a broadcast IP address of a network AND the packet not being network administration traffic AND the packet not having a protocol listed in a list of protocols previously determined to be harmless network broadcast traffic, to determine and report that the packet is a new, exploit candidate.

10. (Currently Amended) A computer program product for automatically determining if a packet is a new, exploit candidate, the computer program product comprising:

a computer-readable tangible storage device;

first program instructions to determine if the packet is a known exploit;

second program instructions to determine if the packet is addressed to a broadcast IP address of a network;

third program instructions to determine if the packet is network administration traffic;

fourth program instructions, responsive to the packet being a known exploit OR the packet being addressed to a broadcast IP address of a network OR the packet being network administration traffic, to determine that the packet is not a new, exploit candidate; and

fifth program instructions, responsive to the packet not being a known exploit AND the packet not being addressed to a broadcast IP address of a network AND the packet not being network administration traffic AND the packet not being another type of traffic known to be benign, to determine and report that the packet is a new, exploit candidate; and wherein

the first, second, third, fourth and fifth program instructions are stored on the computer-readable tangible storage device; and

~~The computer program product of claim 1 wherein~~ the third program instructions determine if the packet is network administration traffic by comparing an IP protocol and IP address of the packet to a list of combinations of IP protocols and IP addresses previously determined to be network administration traffic.

11. (Currently Amended) A computer program product for automatically determining if a packet is a new, exploit candidate, the computer program product comprising:

a computer-readable tangible storage device;

first program instructions to determine if the packet is a known exploit;

second program instructions to determine if the packet is addressed to a broadcast IP address of a network;

third program instructions to determine if the packet is network administration traffic;

fourth program instructions, responsive to the packet being a known exploit OR the packet being addressed to a broadcast IP address of a network OR the packet being network administration traffic, to determine that the packet is not a new, exploit candidate; and

fifth program instructions, responsive to the packet not being a known exploit AND the packet not being addressed to a broadcast IP address of a network AND the packet not being network administration traffic AND the packet not being another type of traffic known to be benign, to determine and report that the packet is a new, exploit candidate;

sixth program instructions to determine if the packet is web crawler traffic; and wherein

the fourth program instructions are responsive to the packet being a known exploit OR the packet being addressed to a broadcast IP address of a network OR the packet being network administration traffic OR the packet being web crawler traffic, to determine that the packet is not a new, exploit candidate; and

the fifth program instructions are responsive to the packet not being a known exploit AND the packet not being addressed to a broadcast IP address of a network AND the packet not being network administration traffic AND the packet not being web crawler traffic, to determine that the packet is a new, exploit candidate; and

the first, second, third, fourth, fifth and sixth program instructions are stored on the computer-readable tangible storage device; and

~~The computer program product of claim 2 wherein~~

the sixth program instructions determine if the packet is web crawler traffic by comparing an IP address of the packet to a list of IP addresses of known web crawlers.

12. (Previously Presented) The computer program product of claim 1 further comprising sixth program instructions, responsive to the packet not being a known exploit AND the packet not being network broadcast traffic AND the packet not being addressed to a broadcast IP address of a network AND the packet not being another type of traffic known to be benign, to identify a sequence of packets including the first said packet, the sequence of packets being a new, exploit candidate; and wherein

the sixth program instructions are stored on the computer-readable tangible storage device.

Claims 13-20 (Canceled)

21. (Previously Presented) A computer program product for automatically determining if a packet is a new, exploit candidate, the computer program product comprising:

a computer-readable tangible storage device;

first program instructions to determine if the packet is a known exploit;

second program instructions to determine if the packet is addressed to a broadcast IP address of a network;

third program instructions to determine if the packet has a protocol listed in a list of protocols previously determined to be harmless broadcast traffic;

fourth program instructions to determine if the packet is network administration traffic;

fifth program instructions, responsive to the packet being a known exploit OR the packet being addressed to a broadcast IP address of a network OR the packet being network administration traffic OR the packet having a protocol listed in a list of protocols previously determined to be harmless broadcast traffic, to determine that the packet is not a new, exploit candidate; and

sixth program instructions, responsive to the packet not being a known exploit AND the packet not being addressed to a broadcast IP address of a network AND the packet not being network administration traffic AND the packet not having a protocol listed in a list of protocols previously determined to be harmless broadcast traffic, to determine and report that the packet is a new, exploit candidate; and wherein

the first, second, third, fourth, fifth and sixth program instructions are stored on the computer-readable tangible storage device.

22. (Previously Presented) The computer program product of claim 21 further comprising:

seventh program instructions to determine if the packet is web crawler traffic; and wherein

the fifth program instructions are responsive to the packet being a known exploit OR the packet being addressed to a broadcast IP address of a network OR the packet being network administration traffic OR the packet being web crawler traffic OR the packet having a protocol listed in a list of protocols previously determined to be harmless broadcast traffic, to determine that the packet is not a new, exploit candidate; and

the sixth program instructions are responsive to the packet not being a known exploit AND the packet not being addressed to a broadcast IP address of a network AND the packet not being network administration traffic AND the packet not being web crawler traffic AND the packet not being other traffic known to be benign AND the packet not having a protocol listed in a list of protocols previously determined to be harmless broadcast traffic, to determine that the packet is a new, exploit candidate; and

the seventh program instructions are stored on the computer-readable tangible storage device.

23. (Previously Presented) The computer program product of claim 21 further comprising:

seventh program instructions, responsive to the sixth program instructions determining that the packet is a new, exploit candidate, to determine a signature of the packet or a sequence of packets including the first the packet, and report the new, exploit candidate and the signature to an administrator; and wherein

the seventh program instructions are stored on the computer-readable tangible storage device.

24. (Previously Presented) The computer program product of claim 21 wherein the second program instructions determine if the packet is addressed to a broadcast IP address of the network by comparing a destination IP address of the packet to a gateway IP address of the network and a netmask of the network which identifies a broadcast IP address of the network.

25. (Previously Presented) A computer system for automatically determining if a packet is a new, exploit candidate, the computer system comprising:

one or more processors, one or more computer-readable memories, one or more computer-readable tangible storage devices, and program instructions stored on at least one of the one or more storage devices for execution by at least one of the one or more processors via at least one of the one or more memories, the program instructions comprising:

first program instructions to determine if the packet is a known exploit;

second program instructions to determine if the packet is addressed to a broadcast IP address of a network;

third program instructions to determine if the packet is network administration traffic;

fourth program instructions, responsive to the packet being a known exploit OR the packet being addressed to a broadcast IP address of a network OR the packet being network administration traffic, to determine that the packet is not a new, exploit candidate; and

fifth program instructions, responsive to the packet not being a known exploit AND the packet not being addressed to a broadcast IP address of a network AND the packet not being network administration traffic AND the packet not being another type of traffic known to be benign, to determine and report that the packet is a new, exploit candidate.

26. (Previously Presented) The computer system of claim 25 further comprising:

sixth program instructions, stored on at least one of the one or more storage devices for execution by at least one of the one or more processors via at least one of the one or more memories, to determine if the packet is web crawler traffic; and wherein

the fourth program instructions are responsive to the packet being a known exploit OR the packet being addressed to a broadcast IP address of a network OR the packet being network administration traffic OR the packet being web crawler traffic, to determine that the packet is not a new, exploit candidate; and

the fifth program instructions are responsive to the packet not being a known exploit AND the packet not being addressed to a broadcast IP address of a network AND the packet not being network administration traffic AND the packet not being web crawler traffic, to determine that the packet is a new, exploit candidate.

27. (Previously Presented) The computer system of claim 25 wherein the packet was received by a honeypot computing device at an unused IP address, and the first, second, third, fourth and fifth program instructions are executed at the honeypot computing device.

28. (Previously Presented) The computer system of claim 25 further comprising:

sixth program instructions, stored on at least one of the one or more storage devices for execution by at least one of the one or more processors via at least one of the one or more memories, responsive to the fifth program instructions determining that the packet is a new exploit candidate, to determine a signature of the packet, and report the new exploit candidate and the signature to an administrator.